REMARKS

Claims 1-32 are pending in the present application. Claims 2-4 and 19-21 have been canceled and claims 1, 5-7, 9-11, 13, 14, 16-18, 22-24, 26-28, and 30-31 have been amended. Reconsideration of the claims is respectfully requested.

Amendments to the specification have been made to correct typographical errors that were not noticed until after filing of the application.

I.   35 U.S.C. § 102, Anticipation

Claims 1-32 stand rejected under 35 U.S.C. 102(b) as being anticipated by "Internet Authentication Service for Windows 2000" hereafter referred to as IAS. This rejection is respectfully traversed.

The rejection states,

> IAS teaches a method for integrating a plurality of servers comprising:
> • Transmitting an authentication request from a first server to authenticate a user in a database registry / the NAS forwards the authentication request to an IAS server in the form of a RADIUS Access-Request packet (Page 8, Line 16, IAS)
> • Authenticating the user in the database registry I Directory contains user account data (Page 8, Fig 1, IAS)
> • First server constructing a credential of the user I The IAS server verifies that the RADIUS Access-Request packet is sent from a configured RADIUS client by checking the source P address. If the Access-Request packet was sent by a valid RADIUS client and digital signatures are enabled for the RADIUS client, the digital signature in the packet is checked using the shared secret (Page 8, Lines 18-22, IAS). User information is transmitted though the NAS placed in an access request packet can be interpreted as constructing a credential of the user.
> Accessing a resource from a second server based on the credential of the user and a protection policy applied to the resource in an object name space associated with' the first server I User attempts to connect to a network (resource) associated with first server (NAS) (Page 8, Line 9, IAS)

The claims have been amended to more clearly recite the invention.

Representative claim 1 now recites,

> 1.   (Amended) A method for sharing registry information among a plurality of heterogeneous servers, comprising the steps of:
>   creating a database registry such that registry information is separated into first registry information that is common to a plurality of applications running on said plurality of heterogeneous servers and second registry information that is specific to ones of said plurality of applications, wherein said first registry information is stored in a common registry and said second registry information is stored in respective second registries associated with respective applications;
>   responsive to receiving a request to authenticate a user in said database registry, constructing a credential of the user; and
>   selectively allowing access to a resource based on the credential of the user

> and a protection policy applied to the resource in an object name space associated
> with a first server of said plurality of users.

Most notably, a recitation has been added regarding the database registry for the plurality of servers, in which information that is common to all applications is stored in a common registry and information that is specific to an application is stored in a respective registry for that application. It is submitted that breaking up the registry information paves the way for registry information to be shared across a number of disparate applications and servers.

The cited sections of IAS states,

> When a user attempts to connect to a network through a dial-up connection or virtual private network, the authentication request is processed as follows:
> 1. The NAS attempts to negotiate a connection with the remote access client by using the most secure protocol first and then the next most secure protocol, continuing to the least secure protocol. For example, a Windows 2000 remote access server tries to negotiate EAP, MS-CHAP v2, MS-CHAP, CHAP, SPAP, and lastly PAP.
> 2. The NAS forwards the authentication request to an IAS server in the form of a RADIUS Access-Request packet.
> 3. The IAS server verifies that the RADIUS Access-Request packet is sent from a configured RADIUS client by checking the source IP address. If the Access-Request packet was sent by a valid RADIUS client and digital signatures are enabled for the RADIUS client, the digital signature in the packet is checked using the shared secret. A shared secret is a text string that serves as a password between the RADIUS server and the RADIUS clients connected to it. Each IAS server must have a shared secret for each NAS or other IAS server that forwards RADIUS requests to it. There are a few rules to note when setting up a shared secret:
> • It must be exactly the same at both servers.
> • It is case-sensitive.
> • It can contain any standard alphanumeric characters or any special characters.[1]

It is submitted that IAS does not appear to disclose the use a registry in which portions of the registry that are common to all of the application servers are stored in a single registry and portions of the registry that are specific to an application are stored in separate, individual registries. Rather, IAS appears to share all information in common. Thus, while IAS provides a verification of users, it is not done in the same manner as is the presently claimed invention.

Thus, it is submitted that the independent claims, all of which contain similar limitations, should be allowed. Further, since claims 5-15 depend from claim 1 and claims 22-32 depend from claim 18, the same distinctions exist between IAS and the

---

[1] IAS, page 8, lines 9-30

claimed invention in claim 1 for these claims. Additionally, a number of the dependent claims claim additional combinations of features not suggested by the reference.

For example, dependent claims 7 and 24 each recite that "*access to the database registry must go through an adapter*". Use of an adapter provides not only flexibility, but also protection for the contents of the registry.

For another example, claims 11 and 28 each recite that "*said respective second database is a meta-data database*". IAS does not appear to refer to the use of a meta-data database in regard to the registry.

Similarly, claims 15 and 32 each recite that "*the first database is a registry database and the second database is a meta-data database*".

Consequently, it is respectfully urged that the rejection of claims 1-32 have been overcome.

Furthermore, IAS does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. Absent the examiner pointing out some teaching or incentive to implement a separation of the registry into shared and unshared portions in IAS, one of ordinary skill in the art would not be led to modify IAS to reach the present invention when the reference is examined as a whole. It is submitted that this rejection is overcome.
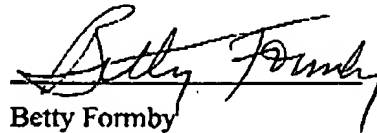
II. Conclusion

It is respectfully urged that the subject application is patentable over IAS and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: May 10, 2005

Respectfully submitted,

Betty Formby
Reg. No. 36,536
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
AGENT FOR APPLICANTS